REQUEST FOR QUOTATION
(THIS IS NOT AN ORDER)

THIS RFQ ☐ IS ☒ IS NOT A SMALL BUSINESS SET ASIDE

PAGE 1 OF PAGES 76

1. REQUEST NO.	2. DATE ISSUED	3. REQUISITION/PURCHASE REQUEST NO.	4. CERT. FOR NAT. DEF. UNDER BDSA REG. 2 AND/OR DMS REG.1	RATING
HSSCCG-10-Q-00025	10/15/2009			

5a. ISSUED BY
USCIS Contracting Office
Department of Homeland Security
70 Kimball Avenue
South Burlington VT 05403

6. DELIVERY BY *(Date)*

7. DELIVERY ☒ FOB DESTINATION ☐ OTHER *(See Schedule)*

9. DESTINATION

a. NAME OF CONSIGNEE
Office of Field Operations

b. STREET ADDRESS
20 Mass. Ave NW, 1st Floor
Attn: Mark Jeanmaire

c. CITY
Washington

d. STATE DC

e. ZIP CODE 20529

5b. FOR INFORMATION CALL: *(No collect calls)*

NAME	TELEPHONE NUMBER: AREA CODE	NUMBER
Steven Putnam	802	872-4111

8. TO:

a. NAME

b. COMPANY

c. STREET ADDRESS

d. CITY

e. STATE

f. ZIP CODE

10. PLEASE FURNISH QUOTATIONS TO THE ISSUING OFFICE IN BLOCK 5a ON OR BEFORE CLOSE OF BUSINESS *(Date)*
10/29/2009 1600 ET

IMPORTANT: This is a request for information, and quotations furnished are not offers. If you are unable to quote, please so indicate on this form and return it to the address in Block 5a. This request does not commit the Government to pay any costs incurred in the preparation of the submission of this quotation or to contract for supplies or services. Supplies are of domestic origin unless otherwise indicated by quoter. Any representations and/or certifications attached to this Request for Quotations must be completed by the quoter.

11. SCHEDULE *(Include applicable Federal, State and local taxes)*

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)
	ALL PRICING PROVIDED SHALL BE IN ACCORDANCE WITH THE TERMS AND CONDITIONS OF THE CONTRACTOR'S RESPECTIVE DHS FIRSTSOURCE CONTRACT. A FIRM-FIXED PRICED DELIVERY ORDER WILL BE ISSUED FROM THIS SOLICITATION.				
0001	Biometric (Live-Scan) Capture Systems, Cabinet Version - Provide systems, install systems and provide onsite user training, and Operations and Maintenance support of systems as specified in the Statement of Work. All locations for delivery, install and training are in Attachment A. Continued ...	400	EA		

12. DISCOUNT FOR PROMPT PAYMENT

a. 10 CALENDAR DAYS (%)	b. 20 CALENDAR DAYS (%)	c. 30 CALENDAR DAYS (%)	d. CALENDAR DAYS NUMBER	d. CALENDAR DAYS PERCENTAGE

NOTE: Additional provisions and representations ☐ are ☐ are not attached

13. NAME AND ADDRESS OF QUOTER

a. NAME OF QUOTER

b. STREET ADDRESS

c. COUNTY

d. CITY

e. STATE

f. ZIP CODE

14. SIGNATURE OF PERSON AUTHORIZED TO SIGN QUOTATION

15. DATE OF QUOTATION

16. SIGNER

a. NAME *(Type or print)*

b. TELEPHONE AREA CODE

NUMBER

c. TITLE *(Type or print)*

AUTHORIZED FOR LOCAL REPRODUCTION
Previous edition not usable

STANDARD FORM 18 (REV. 6-95)
Prescribed by GSA - FAR (48 CFR) 53.215-1(a)

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
0002	Biometric (Live-Scan) Capture Systems, Desktop Version - Provide systems, install systems and provide onsite user training, and Operations and Maintenance support of systems as specified in the Statement of Work. All locations for delivery, install and training are in Attachment A.	100	EA		
0003	Biometric (Live-Scan) Capture Systems, Laptop (Mobile) Version - Provide systems, install systems and provide onsite user training, and Operations and Maintenance support systems as specified in the Statement of Work. All locations for delivery, install and training are in Attachment A.	100	EA		
0004	Disposal of existing Biometric (Live-Scan) systems in conjunction with the installation of the new Live-Scan systems at all USCIS locations specified in Attachment A and in accordance with the Statement of Work.	602	EA		
1001	Option Period 1 - Biometric (Live-Scan) Capture Systems, Cabinet Version - Provide systems, install systems and provide onsite user training, and Operations and Maintenance support of systems as specified in the Statement of Work. All locations for delivery, install and training are in Attachment A. (Option Line Item)	40	EA		
1002	Option Period 1 - Biometric (Live-Scan) Capture Systems, Desktop Version - Provide systems, install systems and provide onsite user training, and Operations and Maintenance support of systems as specified in the Statement of Work. All locations for delivery, install and training are in Attachment A. (Option Line Item)	10	EA		
1003	Option Period 1 - Biometric (Live-Scan) Capture Systems, Laptop (Mobile) Version - Provide systems, install systems and provide onsite user training, and Operations and Maintenance support systems as specified in the Statement of Work. All locations for delivery, install and training	10	EA		

Continued ...

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	are in Attachment A. (Option Line Item)				
1004	Option Period 1 - Operations and Maintenance Support (O&M) for Biometric (Live-Scan) Equipment - Cabinet Type Biometric System, as detailed in the Statement of Work. (Option Line Item)	400	EA		
1005	Option Period 1 - Operations and Maintenance Support (O&M) for Biometric (Live-Scan) Equipment - Desktop Type Biometric System, as detailed in the Statement of Work. (Option Line Item)	100	EA		
1006	Option Period 1 - Operations and Maintenance Support (O&M) for Biometric (Live-Scan) Equipment - Laptop (Mobile) Type Biometric System, as detailed in the Statement of Work. (Option Line Item)	100	EA		
2001	Option Period 2 - Biometric (Live-Scan) Capture Systems, Cabinet Version - Provide systems, install systems and provide onsite user training, and Operations and Maintenance support of systems as specified in the Statement of Work. (Option Line Item)	40	EA		
2002	Option Period 2 - Biometric (Live-Scan) Capture Systems, Desktop Version - Provide systems, install systems and provide onsite user training, and Operations and Maintenance support of systems as specified in the Statement of Work. (Option Line Item)	10	EA		
2003	Option Period 2 - Biometric (Live-Scan) Capture Systems, Laptop (Mobile) Version - Provide systems, install systems and provide onsite user training, and Operations and Maintenance support systems as specified in the Statement of Work. (Option Line Item)	10	EA		
2004	Option Period 2 - Operations and Maintenance Support (O&M) for Biometric (Live-Scan) Equipment - Cabinet Type Biometric System, as detailed in the Statement of Work. (Option Line Item)	400	EA		
2005	Option Period 2 - Operations and Maintenance Support (O&M) for Biometric (Live-Scan) Equipment - Desktop Type Biometric System, as detailed in Continued ...	100	EA		

NAME OF OFFEROR OR CONTRACTOR

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	the Statement of Work. (Option Line Item)				
2006	Option Period 2 - Operations and Maintenance Support (O&M) for Biometric (Live-Scan) Equipment - Laptop (Mobile) Type Biometric System, as detailed in the Statement of Work. (Option Line Item)	100	EA		

STATEMENT OF WORK

UNITED STATES CITIZENSHIP & IMMIGRATION SERVICES (USCIS) Application Support Center (ASC) BIOMETRICS (LIVE-SCAN) REFRESH

September 30, 2009

1.0 Title of Project

USCIS ASC Biometric (Live-Scan) Refresh

2.0 Period of Performance

The period of performance for this delivery order consists of a one year base period and two consecutive one year options. The base period will cover the replacement of the 602 existing biometric capturing systems (to include disposal of old equipment and delivery and installation of the new equipment), also the first year Operations & Maintenance (O&M) support will be provided as part of the new equipment purchased. In option years one and two, continued O&M support will be provided. Also, in the option years, additional Live-Scan Systems may be purchased up to a maximum of 60 units per year.

3.0 Contacts

The Contracting Officer at time of award will appoint a Contracting Officer Technical Representative (COTR) and furnish appointment information to the contactor.

4.0 Background

The United States Citizenship and Immigration Services (USCIS) utilizes Live-Scan electronic fingerprint scanning systems to digitally capture and electronically submit applicant fingerprint images to the Federal Bureau of Investigation (FBI) and US-VISIT. The fingerprints are used to conduct criminal background checks prior to USCIS making a determination whether to grant immigration benefits to applicants. Live Scan systems are currently at approximately 134 USCIS Application Support Centers (ASCs) located throughout the United States and the U.S. territories of Saipan, Guam, the Virgin Islands, and Puerto Rico. In 2001, in response to increased applicant workload resulting from the Legal Immigration Family Equity (LIFE) Act, USCIS initiated collection of digital photographs and digital signatures at the ASCs to further streamline and reduce timeframes needed to process USCIS benefits applications. Live-Scan systems acquired under this delivery order are expected to be used predominately at domestic ASCs and other domestic USCIS sites to replace existing Live-Scan technology that has become worn and outdated. Deployment of Live Scan devices and applicable support to overseas sites may be required under this delivery order, and is considered to be within scope. The existing live scan systems are to be replaced by newer model Live-Scan systems (approximately 400 "cabinet" style machines, 100 "desktop" style machines, and 100 "mobile" style machines) in early 2010. As new systems are deployed at each site, the old systems must be de-installed and disposed. USCIS intends for the contractor to dispose of 602 live scan systems at the ASC sites. This solution will continue to support USCIS' biometrics capturing goals of:

- Improving efficiencies,
- Preventing fraud,
- Ensuring accurate biographic/demographic data,
- Validating the biometrics data, and
- Meeting FBI image quality standards.

5.0 Scope

A description of the application process and the USCIS operating environment and resources available to the Contractor is provided below. Based on the current environment, the Contractor shall provide a turn-key Live-Scan system that can be connected to the USCIS LAN/WAN and which includes all the turn-key Live-Scan components and configurations to meet the operational requirements of this SOW. Live-Scan systems and components must have "plug and play" capability to capture and transmit FD-258 type 14 and type 4 fingerprint impressions, biographic and demographic data, and digital signatures in standard TIFF image format, and Joint Photographic Experts Group (JPEG) photograph images. As Citizenship and Immigration Services' requirements evolve, the Live-Scan systems provided under this delivery order shall be capable of capturing and transmitting additional biometrics data (e.g., iris, pressed 2-print images, etc.) with minor component and configuration changes, if required by the Government. The Contractor shall also provide, as a minimum, Live-Scan system hardware and software installation and integration services, remote VPN software maintenance, remedial hardware maintenance, technical support (toll-free telephone hotline), training (on-site user/ on-site systems administrator), standard commercial warranty, shipping, and removal/disposal of old equipment. The Contractor shall furnish all necessary personnel, materials, and other supplies/services as may be required to perform the work set forth in this SOW.

5.1 Current Environment

USCIS collected biometrics data from 2.5 million immigration benefits applicants in Fiscal Year 2009, of which approximately 1 million required ten-print fingerprinting and the remainder required collection of single flat impression (press) fingerprints, photographs, and digital signatures. USCIS will continue to use Live-Scan systems for electronic submission of FD-258 fingerprint images to the FBI and US-VISIT for use in searching criminal history databases for records that may disqualify an applicant for benefits. USCIS currently operates 602 Live-Scan devices at 134 ASC sites. **Attachment A** lists current ASC sites. Site locations are subject to change by the Government and the contractor will be notified via modification of specific location changes. Some location changes may require placement of equipment at overseas locations. These overseas locations, when added, will require O&M support. When the government requires relocation of Live Scan systems provided under this delivery order, the government may require the contractor to accomplish the equipment relocation. Any changes to the Live-Scan locations will be conducted through a contract modification and negotiated separately.

Live-Scan systems installed at ASCs will be interfaced to Government-provided store-and-forward mail servers, which in turn interface with USCIS Service Centers. The USCIS Service

Centers are the connectivity points to the Criminal Justice Information System (CJIS) WAN for submitting fingerprints and other biometrics data to the FBI, US-VISIT's IDENT, as well as interfacing with other internal USCIS systems. The ASCs use static Internet Protocol (IP) addresses that require Live-Scan Contractor personnel to maintain and change IP addresses in the field in coordination with the USCIS Help Desk.

The process for capturing biometrics data for immigration benefits is as follows (see **Attachment C** for diagram): The applicant submits an application to USCIS to request an immigration benefit. Application requirements vary for each specific benefit, and therefore require different biometrics collection requirements. Depending on the application being processed, USCIS generates either a 1D bar coded or 2D bar coded scheduling notice informing the applicant where and when to go to get processed for benefits. A 2D barcode is usually generated when FD-258 ten-print processing is required, and a 1D barcode is usually generated when only single press prints, photographs, and signatures are required. When notified, the applicant will go to an ASC to have fingerprints, photographs, signatures, and potentially other data captured using Live-Scan technology.

The normal data capture at the ASCs involves the Live-Scan system operator collecting biographic and demographic data including USCIS-specific identification numbers, name, date of birth, social security number, and other data, either by scanning the scheduling notice 1D or 2D barcode to populate the Live-Scan device data fields, using pull-down menus, or by manually entering the data using the keyboard. Current immigration benefits application requirements call for one of the following scenarios: the application requires FD-258 fingerprints (ten-prints) only; the application requires photograph, single press print (optional), and signature (optional) only; or, the application requires ten-print, photograph, single press fingerprint (optional), and signature (optional).

FD-258 fingerprints (ten-prints) taken at individual Live-Scan devices are forwarded in an Electronic Fingerprint Transmission Specification (EFTS) v7.0 compliant transaction to the local ASC store-and-forward mail server. EFTS is a National Institute of Standards and Technology (NIST) standard used by the law enforcement community (local, state, and federal) and civilian agencies to transmit demographic and image files using a common format. If required, a single press fingerprint image that meets FBI image quality standards is captured of the right index finger, or other finger if necessary. A digitally captured signature in standard TIFF image format is then recorded into the Live-Scan system followed by a facial photograph in standard JPEG image compression format. All the data and images captured can be reviewed and updated at the Live-Scan device before accepting and transmitting to the ASC mail server.

From the local store-and-forward mail server, the EFTS formatted applicant data files (biographic/demographic masthead data and EFTS formatted FD-258 ten-print images) are transmitted to the applicable USCIS Service Center. The Service Center server electronically sends all EFTS formatted applicant data files to the FBI. Applicant data files that include a photograph, press fingerprint, signature image, and associated biographic data are sent to the applicable USCIS service center.
The local ASC mail servers store the EFTS formatted applicant data file records for up to 30 days for reporting and resubmission. Each Live-Scan device currently deployed has minimum

capacity to store and retrieve at least 300 EFTS formatted applicant data files. (Note – This SOW requires a minimum storage and retrieval capacity of 500 each of FD-258 Ten-print files and Biometrics Capture files (total is 1,000). The primary objective of the storage of biometrics on the capture devices is to ensure continuity of operations and not to provide a fail safe for biometric data that gets lost in transmission in the store and forward process.

Neither the Live-scan device nor the local store-and-forward mail server communicates directly with the FBI.

ASC personnel are a mix of Government and contracted labor trained in the taking of quality fingerprints through Live-Scan and manual methods. ASC staffs are non-technical: the level of computer knowledge and abilities of the staff varies from location to location, but is generally very limited. The Live-Scan Contractor is advised that tasks including basic Live-Scan equipment set-up/configuration, basic computer file maintenance, account management, calibrating of systems, basic and preventive maintenance, installation of hardware components, etc. are not within the functional areas and technical abilities required of the ASC staff.

6.0 Live-Scan System Requirements

6.1 FBI Certification

All Live-Scan systems and components delivered by the Contractor shall be capable of transmitting FBI NIST/EFTS images to a local store-and-forward server. Live-Scan systems and components provided under this contract shall be FBI certified to comply with the FBI's Integrated Automated Fingerprint Identification System (IAFIS) Image Quality Specifications (IQS) (See Appendix F) and the US-VISIT IDENT System.

6.2 Functional Requirements

The Live-Scan systems provided by the Contractor shall meet all the functional requirements in Section 6.2 and its sub-sections.

6.2.1 FD-258 Ten-Print Capture Requirements

The Live-Scan system:

- Shall process a minimum of six (6) ten-print applicants per hour (i.e., total time for a skilled fingerprint technician to process one FD-258 applicant shall be 10 minutes or less). The process begins when the Live-Scan system scans the 2D bar code with its scanner, entering FD-258 biographic and demographic masthead data, and ends with the submission of the record to the local store-and-forward mail server.
- Shall create an EFTS transaction containing 14 fingerprint images and biographic masthead data.

The applicant data files transmitted by the Live-Scan system to the local store-and-forward mail server shall include: (a) biographic and site operations text data,

and (b) Wavelet Scalar Quantization (WSQ) compressed fingerprint images (14 blocks) corresponding to fingerprint boxes on the applicant fingerprint card.

The applicant data shall include name, date of birth, sex, race, height, weight, eye and hair color, place of birth, residence, country of citizenship, and all other applicable biographic and demographic data as contained in the masthead of the FD-258 Fingerprint Card. Site operations data shall include fields such as an ASC site identifier; machine code, operator code, and Live-Scan make and model. Text data fields shall conform to EFTS v7.0. Information that populates the EFTS standard will be provided to the vendor after award of the delivery order.

Currently, the fingerprint image records shall include the ten rolled fingerprints, two flat impressions of four fingers (left and right hands) and two flat thumb prints. The image sizes shall be consistent with the fingerprint boxes on the standard FD-258 fingerprint card. The transmitted fingerprint images shall be in compliance with ANSI/NIST Standards identified in the attached FBI Appendix F. The compression algorithms used in the Live-Scan system for compressing the fingerprint images must comply with FBI approved WSQ gray scale compression standards.

- Shall support EFTS v7.0 specifications for maximum sizes of fingerprint images (provided in Table C-2).

Fingerprint	**Width Pixels (inches)**	**Height Pixels (inches)**
Rolled impressions Fingers 1 – 10	800 (1.6)	750 (1.5)
Plain Thumb impression	500 (1.0)	1000 (2.0)
4 Finger Plain impression	1600 (3.2)	1000 (2.0)

Table C-2 Maximum Sizes for Fingerprint Images

- Shall support transmission of an EFTS v7.0 file format fingerprint image to the local store-and-forward mail server. **Attachment B** lists typical USCIS server configurations. All the data files shall be transferred to a specified directory on the mail server. All the data files transmitted by the Live-Scan systems shall comply with all applicable FBI, ANSI/NIST and NIST/EFTS standards for the data interchange.

- Shall create and support transmission of an EBTS 8.001 XML file.

- Shall meet the basic format requirements for Logical Record types as defined by the EBTS message set forth in the ANSI standards which are also applicable to transmissions to the FBI.

- Shall create an alpha/numeric identification number in a specified FD-258 field in the event that the applicant does not have either an A-number or a social security

number. The alpha/numeric identification number will consist of a unique applicant identifier appended with a 12-digit date and time stamp in the format CCYYMMDDHHMM. The unique applicant identifier may be a "Z number", which is a 10-digit number generated randomly by the Live-Scan device, an "F number", which is a manually entered number with F in the first position followed by nine numeric numbers, or another unique number specified by USCIS.

- Shall store and transmit a unique site code on each submission in a FD-258 field specified by USCIS.
- Shall read both 1D and 2D bar codes.
- Shall capture type 14 and type 4 fingerprints.
- Shall be capable of capturing quality (FBI-acceptable) fingerprint images for a complete spectrum of skin pigmentation.
- Shall be capable of performing data entry of demographic information using pull down menus/tables.
- Shall be capable of performing instant preview and editing capabilities.
- Shall capture information used for quality control (QC) checks (user ID of the QC checker).
- Shall capture management information to include processing time (date and time stamp for start time and stop time for each applicant record) by machine and by operator, and for each applicant, number of reprints or rejects by machine and by operator. This management data shall, at a minimum, be saved to an ASCII text file and sent to the store-and-forward mail server or other devices.
- Shall have the capacity to store a minimum of 500 ten-print fingerprint records in each machine and 500 biometric records.
- Shall have the capability to purge records from the Live-Scan system upon demand by the user.
- Shall have the capability at the Live-Scan device to query the records stored in the Live-Scan device on an applicant's name, A-number, social security number, or date fingerprinted, and retrieve records and fingerprints (that have not been purged).
- Shall be capable of displaying retrieved records and fingerprints at the Live-Scan device.
- Shall have the capability to edit, modify, and resubmit retrieved records that replace the modified record.

6.2.2 Requirements for Other Biometrics Capture

This subsection specifies requirements for non-tenprint Biometric Capture Only (Single Pressed Print, Photograph, and Signature)

The Live-Scan system:

- Shall process a minimum of six (6) non-tenprint applicants per hour (i.e., total time for a skilled technician to process one applicant shall be 10 minutes or less.) The process begins when the Live-Scan system scans the 2D bar code with its scanner, entering biographic and demographic data, captures a single press fingerprint image, a digital signature, and a digital facial photograph, and ends with the submission of the record to the local store-and-forward mail server.

- Shall allow specified biographic data fields to be entered through the use of 1D and 2D bar code scanners/light pens.

- Shall capture an applicant's signature using a digital signature pad.

- Shall allow the single press-print image and/or digital signature capture to be optional.

- Shall require the digital photograph capture of a single facial photo per record for applicants whose press print, photo and signature are captured.

- The digital camera shall be controlled using the fingerprinting station's keyboard and will utilize face detection software that locates an applicant's face and automatically centers it in the photo. The photo shall be automatically sized to 300 pixels x 300 pixels and saved in the jpeg format.

- Shall create a file containing one facial photograph, biographic data, and an optionally captured digital signature and/or single press fingerprint image.

- The applicant data files transmitted by the Live-Scan system to the local store-and-forward mail server shall include: (a) demographic and site operations data (b) Wavelet Scalar Quantization (WSQ) compressed fingerprint images (one block), (c) FAX4 compressed signature image, and (d) JPEG compressed facial photographic image.

- The applicant data shall include name, alien registration number, social security number and other applicable biographic and demographic data as directed by the ASC Program. Site operations data shall include fields such as an ASC site code, machine code, operator id, and Live-Scan make and model. Text data fields shall conform to EFTS v7.0. Information that populates the EFTS standard will be provided to contractor by the Government after award of the delivery order.

- Shall produce a single press fingerprint .wsq image with maximum dimensions 500 pixels (1.0 inch) wide by 500 pixels (1.0 inch) high.

- Shall support transmission to the local store-and-forward mail server of fingerprint images that meet FBI image quality standards. All the data files transmitted by the Live-Scan systems shall comply with all applicable FBI, ANSI/NIST and NIST/EFTS standards for the data interchange.

- The Live-Scan System shall create an alpha/numeric identification number called a Transaction Control Number (TCN) on each submission in a field specified by the Government. The TCN shall consist of a receipt number (3 alpha characters, 10 numerics) followed by a zero, and followed by a date CCYYMMDD.

- Shall store and transmit a unique site code on each submission in a field specified by the ASC Program.

- The Live-Scan System shall be capable of performing data entry of demographic information using pull down menus. Data entry shall be done using touch screen displays to speed up the processing of the masthead data.

- Shall be capable of performing instant preview and editing capabilities.

- Shall capture management information to include processing time (date and time stamp for each applicant record) by machine and by operator. This management data shall, at a minimum be sent to the store-and-forward mail server.

- Each applicant record shall include demographic data; one JPEG compressed photograph image; one optionally captured fingerprint; and one optionally captured signature.

6.2.3. Technical Requirements for the Live-Scan System

The Live-Scan system provided by the Contractor shall:

- Comply with all applicable FBI, ANSI/NIST, NIST/EFTS Standards outlined in the FBI Appendix F for the data interchange and list such standards in its documentation.

- Be capable of transmitting records using the latest FBI record format – Electronic Biometric Transmission Specification (EBTS) 8.1 and EBTS 8.001 XML.

- Provide the run time licenses for its local applications (e.g., database).

- Include a standard 1yr warranty or better.

- Incorporate standard system security features (e.g., operator log-on, passwords).

- Use Commercial Off The Shelf (COTS) software to allow for the customization of data entry and menu screens. The COTS software should run on a variety of hardware platforms to ensure all devices have the same look and feel to the operators.

- Use Computer equipment (Workstations, laptops, etc.) that meets USCIS Office of Information Technology (OIT) specifications to ensure a consistent platform across USCIS. The workstations and laptops shall be the same or equivalent (brand name or equal) to:

  The current OIT-Approved Workstation configuration is: a DELL Optiplex 760 Small Form Factor with an Intel Core 2 Duo E7300 2.66 GHz Processor, 4 GB Memory (2 X 2GB Modules), 160 GB Hard Drive, 8x DVD +/-RW Slimline Drive, 256 MB ATI Radeon HD 3450 Dual DVI/VGI Graphics Card with TV-out, Slimline Floppy Disk Drive, and a 10/100/1000 MB Network Interface Card.

  The current OIT-Approved Laptop configuration is: a DELL Precision M6400 with an Intel Core 2 Duo T9550 2.66 GHz Processor, 4 GB Memory (2 X 2GB Modules), 160 GB Hard Drive, 8x DVD +/-RW Drive, 17 inch WUXGA LCD Wide Screen, 9 Cell/85 WHr Primary Battery, 100/1000 MB Network Interface Card, Bluetooth Wireless and 802.11 a/b/g/n Mini-Card, Internal Backlit Keyboard, Internal/External Floppy Disk drive.

- Use an Uninterrupted Power Supply (UPS) that meets USCIS Office of Information Technology (OIT) specifications to ensure a consistent platform across USCIS (applicable to "cabinet" and "desktop" systems). The UPS shall be the same or equivalent (brand name or equal) to:

  The current OIT-Approved UPS is: a Smart Pro LCD UPS with a Network Monitoring USB Port, 4 UPS Battery Support Outlets, and Additional 4, Surge Suppression-Only Outlets.

- Be designed to function in an office environment of 60 to 90 degrees Fahrenheit and 20 to 80 percent relative humidity, non-condensing, and shall not require any special air conditioning.

- Meet or provide equivalent facilitation for applicable Section 508 Electronic and Information Technology Accessibility standards for the disabled (see Section 16.0, Electronic and Information Technology Accessibility).

- Be upgradeable such that it is capable of capturing a variety of biometric data including type 14, type 4 fingerprint images, iris, photos, and signature using plug and play devices.

- Be capable of adjusting the height of the scanner decks, and shall have ngled keyboards to make the fingerprint equipment ergonomic; for ease of use by the fingerprint technicians (pertains to "cabinet" systems).

- Allow fingerprint capture by use of a foot pedal. The Live-Scan Operator shall be able to capture an applicant's fingerprint images by pressing a foot pedal so that he/she has full use of his/her hands to assist in rolling an applicant's fingers for print capture (applicable to "Mobile", "Desktop" and "Cabinet" systems). This requirement may be omitted if the Live-Scan System allows the Live-Scan Operator full use of his/her hands to assist in rolling an applicant's fingers for print capture.

6.2.4. Hardware Configurations

The Live-Scan Systems are comprised of 3 different hardware configurations in the quantities specified in the delivery order schedule:

1. Cabinet System:

- A standalone system that has the computer, uninterrupted power supply, fingerprint scanner, foot pedal, touchscreen monitor, 1D & 2D barcode reader, digital camera, and digital signature pad supported by a "cabinet" structure.
- A stand may be substituted for a cabinet as long as it meets all of the requirements of the cabinet.
- The "cabinet" or stand shall no larger than 30"deep X 24" wide.
- The "cabinet" or stand shall be robust enough to support all of the above mentioned equipment and withstand full-time operational use for a 5yr lifecycle.
- The "cabinet" or stand shall have locking wheels.
- The fingerprint scanner is easily adjustable for height so that scanner can be raised or lowered to fit the height of the fingerprint technicians and to allow for handicapped access.
- The foot pedal rests on the floor and allows the Live-Scan Operator to capture an applicant's fingerprint images by pressing a foot pedal so that he/she has full use of his/her hands to assist in rolling an applicant's fingers for print capture (applicable to "Mobile", "Desktop" and "Cabinet" systems). This requirement may be omitted if the Live-Scan System allows the Live-Scan Operator full use of his/her hands to assist in rolling an applicant's fingers for print capture.
- The camera is affixed to the cabinet to prevent it from being knocked over.
- The keyboard is angled to help prevent injuries to the operators.
- The CPU and UPS shall be located in a locking enclosure to prevent tampering.
- Computer cables are hidden or are secured to avoid entanglement with the operator or applicant.
- Cable connections are secured to prevent damage if the cabinet is moved.
- Components will be plug and play compatible.

2. Desktop System:

- Composition is the same as the cabinet system, excluding the cabinet itself.
- Hardware is capable of being used on existing tables and or system furniture.
- Camera has to be secured to prevent it from being knocked over or knocked out of position.
- Table top version has all the same functionality as the cabinet version except for height-adjustable scanner deck and angled keyboard.
- Components will be plug and play compatible for ease of setup and removal.

3. Mobile System:

- Composition is the same as the cabinet system with the addition of a ruggedized case and the exclusion of the cabinet, UPS, computer (laptop as substitute), touchscreen monitor, height-adjustable scanner deck, and angled keyboard.
- Camera will be secured to a tripod for easy set up.
- Portable system will be capable of being packed into a single contractor-provided ruggedized case for transport. System must be capable of meeting all airline travel requirements.
- External battery power is provided to allow equipment to be operated in remote locations without electricity.
- All devices will be plug and play compatible for ease of setup and removal.
- A portable backdrop will be included for the purposes of capturing photographs

All components, such as the uninterrupted power supply, fingerprint scanner, foot pedal, touchscreen monitor, 1D & 2D barcode reader, digital camera, and digital signature pad, that may require device drivers shall be consistent across all Live-Scan Systems, without deviation in make and model. This ensures a consistent Live-Scan System across USCIS, which is critical for USCIS operating system image configuration.

6.2.5. Software Configurations

The Contractor shall perform all required Live-Scan software configurations/modifications required to interface with USCIS systems and meet USCIS data profile requirements. The Contractor shall submit the modified software for USCIS approval prior to placement on live-scan systems. Immediately following contract award, USCIS will provide the Contractor with the specifications for data fields and types, screen layouts, and the local store-and-forward mail server connection information. The Contractor will then be responsible for customizing its COTS Live-Scan application software and submitting it to USCIS (Attention: Hugh Jordan) for testing and approval. Testing will occur at USCIS HQ (111 Massachusetts Ave, NW, Washington DC, 20001) in the 2nd floor ASC lab.
As part of the software customization, the Contractor shall be required to maintain USCIS software tables that include demographic information used in processing USCIS Live-Scan transactions. Tables are accessed by the Live-Scan operator through the use of pull-down menus on the Live-Scan device. USCIS will provide USCIS-specific tables (e.g., Originating Agency Indicator (ORI) Code, Reason Fingerprinted, Place of Birth, and Country of Citizenship) to the

Contractor after award for incorporation into the Contractor's Live-Scan software. USCIS will validate all tables during the software approval process.

In addition to the USCIS software configurations, the software requires customization for the processing of UKvisas applicants. See **Attachment E** for the customization requirements for UKvisas.

The Live-Scan application must operate on a USCIS-provided Windows XP operating system with the Federal Desktop Core Configuration (FDCC). The National Institute of Standards and Technology (NIST) FDCC guidelines and specifications are available at the following link: http://csrc.nist.gov/itsec/download_WinXP.html

The USCIS operating system "image" will be provided to the contractor upon award of the delivery order. As part of the USCIS image, the software (to include the operating system), corresponding licenses, and maintenance will be provided by the government via Enterprise License Agreements.

The Live-Scan System shall support a Lightweight Directory Access Protocol (LDAP) connector such that the scanner application software utilizes the Microsoft Active Directory for user accounts and login.

7.0 Delivery

The Contractor shall provide the COTR with one central point of contact for all activities related to initial setup and deployment.

The Contractor must provide two (2) of each type of Live-Scan System ("cabinet", "desktop", and "mobile") to USCIS Headquarters (Attention: Hugh Jordan, Office of Field Operations, 111 Massachusetts Avenue, Washington, DC 20001) within five (5) business days following contract award. A business day is defined as Monday – Friday, 8AM to 5PM. The systems shall include all peripherals and the COTS software (if the "cabinet" and "desktop" configurations include identical computers and peripherals, then only one (1) "cabinet" system and one (1) "desktop" system shall need to be provided). These systems will be used for the purpose of systems configuration/compatibility testing and solidifying the USCIS operating system "image" to be used by the Live-Scan Systems.

No later than 28 calendar days after the delivery order award date, all software configurations and testing must be completed and final acceptance by the government must be received. The Contractor will be required to work on-site with USCIS staff at USCIS Headquarters to solidify the customization of the Live-Scan Application and the operating system images (one for each computing platform). Any time saved on the 28 calendar days will also be added to the 100 calendar day deployment schedule (up to 14 calendar days). After final acceptance of the software customization by the government, an additional 14 calendar days will be required to complete the USCIS image. Once complete, the government will provide the Contractor a copy of the USCIS Image. Once the image is provided to the contractor, the deployment period begins.

All 400 "cabinet" and 100 "desktop" Live-Scan Systems Live-Scan Systems shall be operational at all USCIS locations identified in **Attachment A** no later than 100 calendar days from the start of the deployment period. The contractor shall dispose of all old equipment; deliver and install new Live-Scan equipment, perform operational testing, and provide required training at every USCIS location, listed in **Attachment A**, in order for the systems to be considered operational.

"Mobile" Live-Scan Systems will not require installation and training. The 100 mobile systems shall be delivered to the USCIS Sites as specified in **Attachment A**, except for the laptop/computing devices themselves, which shall be shipped to USCIS Headquarters (111 Massachusetts Ave, Washington D.C. 20001) no later than 100 days from the beginning of the deployment period, where the government will install the USCIS operating system image, application software, and deliver them to the USCIS locations. The government will be responsible for the installation of the 100 "mobile" systems.

The deployment schedule is included as **Attachment D**. The contractor is to provide a written deployment plan immediately following contract award addressing the deployment schedule to include the disposal of old equipment, installation of new equipment, and training of users by USCIS Site. (**Attachment A** identifies the quantity and types of Live-Scan Systems to be installed at each USCIS location)

Operations and Maintenance (O&M) Support provided with the purchased equipment shall commence when all Live-Scan Systems are operational. Any installed systems, prior to all systems being operational, shall be supported by the contractor and any service shall be considered part of the installation. Inside delivery will be required for all shipments and curb-side delivery (drop-shipping is not allowed and/or acceptable).

7.1 Shipping

The Live-Scan Systems shall be shipped to arrive at the installation site no sooner than 72hrs prior to installation. Live-Scan Systems shall be shipped as complete systems as opposed to shipping separate components. Live-Scan assembly shall be completed prior to shipment. The operating system and necessary software shall be installed and configured prior to shipment. Shipment dates shall be coordinated with the COTR. Shipping shall be considered FOB Destination and acceptance of the Live-Scan Equipment will occur upon receipt of a G504 Form. Shipping, packaging, and packing materials shall use recycled/recyclable materials to the maximum extent practicable. The Contractor is responsible for removing all shipping, packaging, and packing materials during installation and disposal.

7.2 Milestone Chart

MILESTONE CHART

Milestone	Description	Due Date

1	Deliver 2 of each Live-Scan System model to USCIS HQ (111 Massachusetts Ave, Washington DC 20001)	5 business days after award
2	Submit Final Systems Deployment Plan and Final Program Management Plan	5 business days after award
3	Appoint a senior official to act as the Corporate Security Officer Provide the COTR with one central point of contact for all activities related to initial setup and deployment	5 business days after award
4	Successful completion of Test Phases 1-3. Complete Live-Scan Software Customization	28 calendar days after contract award
5	Prospective Contractor employees shall submit completed background investigation forms to OSI through the COTR	No less than 30 days before the starting date of the contract or 30 days prior to entry on duty of any employees (approx 5 days after award)
6	Submit IT Security Plan for approval	Within 30 calendar days after contract award
7	Favorable entry on duty (EOD) determination received Contractor employees shall submit LAN account and GFE request forms	After favorable entry on duty (EOD) determination (approx 35 calendar days after award)
8	Submit MAC Address List	Prior to systems deployment (approx 36 calendar days after award)
9	USCIS Operating System Image completed and distributed to Contractor	42 calendar days after contract award
10	LAN Accounts and GFE received Begin deployment of Live-Scan Systems	43 calendar days after contract award
11	Complete Computer Security Awareness Training (CSAT)	60-days from the date of entry on duty (EOD)
12	All Live-Scan Systems Fully Operational (mobile unit cases and peripherals deployed and laptops sent to USCIS HQ)	143 calendar days after award
13	End of Deployment Phase & Operations and Maintenance Support begins	144 calendar days after award

8.0 Test and Acceptance

The test and acceptance evaluation shall occur in four (4) phases (and will be performed on the 4-6 systems provided immediately following contract award):

Phase 1 - Acceptance of the customization required of the COTS biometrics software application. The test will ensure all necessary data capture fields and corresponding data entry screens have been added in order to process UKvisas and Code 1-3 applicants. Login and password integration (using an LDAP connector to access the Microsoft Active Directory) will also be tested. Phase 1 requires acceptance no later than 28 calendar days after award date. Testing shall be performed at the USCIS ASC Lab (111 Massachusetts Avenue, 2nd floor, Washington D.C. 20001)

Phase 2 – This tests the communication connection between the Live-Scan system and the local store-and-forward mail server. The test must demonstrate that the fingerprint file generated by the Live-Scan is in the format specified by all relevant standards, compliant with ANSI/NIST and FBI specifications, and stored in the proper directory on the local store-and-forward mail server. Processing an USCIS application will test the file format for acceptability. Phase 2 requires acceptance no later than 28 calendar days after award date. Additionally, at time of installation at each USCIS location, this must be reconfirmed in order for each system to be considered operational. Testing shall be performed at the USCIS ASC Lab (111 Massachusetts Avenue, 2nd floor, Washington D.C. 20001).

Phase 3 - This test provides for acceptance of the encrypted file format and external media (such as a DVD-ROM) format by the Government. The file format originates from the Live-Scan systems and is forwarded to the local store-and-forward mail server, which forwards a daily batch to the Government's applicable store-and-forward transaction manager. Data is written to the external media (such as a DVD-ROM) using the same EFTS 7.0 format as the file format. Phase 3 requires acceptance no later than 28 calendar days after award date. Additionally, at time of installation at each USCIS location, this must be reconfirmed in order for each system to be considered operational.

Phase 4 – This tests the communication connection between the Live-Scan system and the ESB. The test must demonstrate that the fingerprint file generated by the Live-Scan is in the format specified by all relevant standards, compliant with ANSI/NIST and FBI EBTS specifications. Processing a USCIS application will test the file format for acceptability. This phase shall be conducted after deployment, and at the discretion of the Government.

9.0 Disposal

For all systems requiring disposal, the Contractor shall:

a. De-install existing Live-Scan systems in coordination with the installation of the new Live-Scan systems per the deployment schedule. Live scan systems at each specific location are to be disposed of in accordance with this SOW.

b. Remove the hard drive component from the CPU of each Live-Scan system and give the hard drive components to the onsite Desktop Support Manager (DSM). If the onsite DSM is

absent, the ASC Manager or Site Supervisor shall suffice. The Contractor is responsible for providing written proof that the DSM, ASC Manager, or Site Supervisor certified in writing that the hard drive components for each specific machine have been removed and placed in custody of a government representative.

c. Dismantle and haul away each complete Live-Scan system and attached components for disposal as scrap.

d. Complete and Sign Form G-504, Report of Property Shipped/Received. The ASC Manager or Site Supervisor will also sign and take possession of the Form G-504 to acknowledge transfer of scrap property to the Contractor representative.

e. Ensure the following information included on and/or attached to the G-504 for each scrap system is correct:

(1) Live-Scan System Property Control Number (PCN)
(2) Component PCNs, if applicable
(3) Live-Scan System Serial Number
(4) Live-Scan Model Number

f. Remove all DHS PCN Labels from the Live-Scan Equipment and attach them to the back of the G-504. There are typically 3 labels on each Live-Scan system: 1 on the cabinet or computer, 1 on the barcode reader, and 1 on the digital camera.

g. Make all arrangements for transportation and disposal of scrap property, including inside pick- up, truck lift gate, shipping, and payment of disposal facility handling and disposal fees.

h. Ensure that all applicable Environmental Protection Agency (EPA) and state environmental regulations are met in disposing of the scrap property. Components of the scrap equipment contain hazardous materials. Prior to disposal, the Contractor shall obtain written certification and/or other proof from the waste disposal facility that the disposal facility is fully certified for hazardous waste disposal.

i. Following disposal, verify in writing to the ASC Program Contracting Officer Technical Representative (COTR) that the equipment has been disposed of as scrap material through proper waste disposal procedures and facilities in accordance with all applicable government regulations. The Contractor shall provide the information listed in paragraph e, above, to describe the disposed scrap in the scrap disposal verification letter(s).

9.1. Performance of Services: The Contractor shall coordinate the de-installation and removal of scrap Live-Scan systems with the HQ, USCIS ASC Branch and local USCIS ASC/District staff.

9.2. Reselling Prohibition: The Contractor shall not resell any equipment that contains a memory component. Such components shall be disposed of in accordance with MD4300.1.

10.0 Installation

The contractor shall be responsible for all aspects of installation. Installation includes the following activities:

- Install and/or integrate Live-Scan hardware
- Install and/or integrate Live-Scan software, to include the USCIS image (provided by USCIS)
- Install and/or integrate component pieces as required to meet the requirements of this SOW
- Install DHS Property Control Number (PCN) Labels on Live-Scan Systems
- Complete a Form G-504 for the installation at each USCIS site.

The Government is responsible for installation site modifications, if required, to prepare the facility to receive the equipment, to include cabling, wiring, construction, and mail server installation.

The Contractor shall integrate all the hardware and load all necessary software and conduct a complete configuration test sufficient to ensure that the Live-Scan system is fully functional in each USCIS ASC site. The configuration for each ASC Live-Scan system shall be identical. The Contractor shall be responsible for setup and integration of devices. The Contractor shall certify each system as completely operational following installation and integration, in accordance with all terms and conditions of this delivery order.

Installation of the operating system on the fixed-disk drives in its own subdirectory; USCIS will provide the contractor with the USCIS operating system image. The contractor will be responsible for installing the image on each Live-Scan System. The USCIS image (containing the operating system and necessary software) shall be installed and configured prior to installation at a USCIS site.

The Contractor shall, in all cases, be responsible for certification, and delivery of hardware and software not later than the delivery date specified in this delivery order, in accordance with the Schedule. The Contractor shall adequately package Live-Scan systems to prevent shipping damage, make all arrangements for transportation, shipping, insurance, and commercial Bills of Lading, and unpack and install systems at the receiving USCIS fingerprinting locations. Shipping costs shall be included in the price of the Live-Scan systems.

After contract award and prior to deployment, USCIS shall provide the Contractor with approximately 1,800 PCN Labels. While in the care of the Contractor, the Contractor shall be responsible for the PCN labels. The Contractor shall install the PCN labels on the Live-Scan Systems as follows:

Each model ("cabinet", "desktop", and "mobile") shall have a total of 3 PCN Labels:

1) One on the cabinet (if applicable) else on the computer
2) One on the Barcode Reader

3) One on the Digital Camera

Upon successful Live-Scan System installation at a USCIS site, the Contractor shall complete and Sign Form G-504, Report of Property Shipped/Received. The ASC Manager or Site Supervisor will also sign and take possession of the completed Form G-504 to acknowledge transfer of new property to the Government.

The Contractor shall ensure the following information included on the G-504 for each new system is correct:

(1) Live-Scan System Property Control Number (PCN)
(2) Component PCNs, if applicable
(3) Live-Scan System Serial Number
(4) Live-Scan Model Number

11.0 On-Site Training

At the time of installation, the Contractor shall conduct on-site training of all USCIS designated Live-Scan operators. The anticipated total number of individuals requiring initial training is approximately 1,000. Training shall be conducted at each ASC site (**Attachment A**). On-site training includes User training and Site Supervisor training. User Manuals and User Systems Administrators Manuals shall be provided at delivery and reviewed/used to facilitate training.

User Training includes the following:

- Operational instruction to identified Live-Scan operators.
- Review and familiarization with User Manual documentation (e.g., manual, video).
- Instruction on the systems' plug and play capabilities.
- Instruction on the setup and disassembly of portable systems.
- Basic instruction on general maintenance such as calibration and system restart.

Site Supervisor Training includes User Training plus the following activities:

- Basic troubleshooting/depot component replacement.
- Train the trainer instruction.
- Review and familiarization with User Manual documentation (e.g., manual, video).
- Instruction on software setup, if applicable.

12.0 Operations and Maintenance (O&M) Support

12.1 Technical Support Services (Hotline)

The Contractor shall provide a system of technical support for all Live-Scan systems delivered by the Contractor. The Contractor shall provide 24/7 hotline support via a single toll-free number in order to support the following hours of operation:

Sunday	Closed
Monday	7 am – 5 pm (local time at each USCIS site as listed in **Attachment A**)
Tuesday	7 am – 5 pm (local time at each USCIS site as listed in **Attachment A**)
Wednesday	7 am – 5 pm (local time at each USCIS site as listed in **Attachment A**)
Thursday	7 am – 5 pm (local time at each USCIS site as listed in **Attachment A**)
Friday	7 am – 5 pm (local time at each USCIS site as listed in **Attachment A**)
Saturday	Closed

The USCIS Service Desk will use the hotline to report technical problems for all ASC sites. The Contractor shall provide a telephonic response within one (1) hour, at which time a resolution or plan for resolution will be provided.

The Contractor shall provide the most effective method of providing responsive technical troubleshooting and resolution support, to include VPN remote access support. USCIS will provide VPN connections via the use of USCIS-issued laptops and SecureID tokens.

12.2 Remedial and Preventive Maintenance Services

The Contractor shall be responsible for hardware and software maintenance support for Live-Scan systems provided under this delivery order. The Contractor shall provide all maintenance coverage necessary to meet the requirements of this SOW. The Contractor shall coordinate warranty information and warranty services with the manufacturer of the hardware or software. At a minimum, the Contractor shall provide remedial maintenance coverage. Subject to security policies, regulations and procedures, the Government will permit on-site access to the equipment that is to be maintained.

12.2.1 General Maintenance Requirements

The Contractor shall provide all necessary personnel, materials, parts, tools, diagnostic and test equipment, technical manuals/publications and other services as may be required for the hardware maintenance support.

- Maintenance support shall include technical troubleshooting, problem resolution and component repair or replacement in order to maintain and keep the equipment covered under the order in full operating condition.

- The Contractor shall provide data concerning all maintenance activities. A service incident report (SIR) shall be available to the Government for any maintenance rendered by the Contractor under this delivery order (See Section 13.2.1.4. Responsibilities of the Contractor).

12.2.1.1 Periods of Maintenance

The Principal Period of Maintenance (PPM) and Official Operation Hours for equipment covered under this delivery order is 7 a.m. through 5 p.m., local time for each location as identified in **Attachment A**, Monday through Friday (five (5) days per week), excluding Federal Holidays.

12.2.1.2 Software Maintenance

The Contractor shall remotely load all revised software configurations and table updates down to the individual Live-Scan system from a central location utilizing the USCIS issued laptops and SecureID tokens. Remote access to the individual Live Scan systems can only be accomplished through the SecureID VPN token connections. VPN connections via SecureID tokens is the only means of performing certain types of maintenance to include software and hardware maintenance or system troubleshooting.

12.2.1.3 Hardware Maintenance

1. Preventive Maintenance

   Preventive Maintenance is defined as regularly scheduled activities to maintain hardware in full operating condition. The frequency of preventive maintenance shall be at the discretion of the Contractor). The preventative maintenance shall be performed during remedial maintenance calls and/or during a mutually acceptable time during the specified PPM, unless otherwise agreed to by the Contractor and the Government. The Contractor shall provide the Government with a Preventative Maintenance schedule for Government review and approval.

2. Remedial Maintenance

   Remedial maintenance is defined as identifying the source of an equipment or software malfunction and either repairing or replacing the malfunctioned component or subsystem. The Contractor shall provide the parts and equipment required for the diagnosis and repair of malfunctioning components of the Live-Scan system at the most cost effective manner available which will also minimize the downtime of the system. Remedial maintenance shall include transportation, labor and parts required for return of a malfunctioning system or equipment to full operating condition.

   Repaired and/or replaced parts and labor shall be warranted for the standard 1 year warranty period from the date all systems are operational. If additional calls are required during the warranty period, for the warranted repair, they shall be made at no additional cost to the Government. The contractor shall submit a copy of the Live-Scan warranty in writing to the COTR upon award of the delivery order.
   The Contractor's responsibilities for remedial maintenance shall include:

   - The administration and management of all warranties associated with the Live-Scan systems.

- Tracking the status and invoking the use of all applicable warranties of the Live-Scan systems.
- Telephonic responses to the originator within 1 hour of trouble call
- When on-site support is not required, the support must be completed within one (1) business day or three (3) business days if the shipping of parts is required.
- When on-site support is required, the support must be completed within three (3) business days for ASCs located within the Contiguous United States.
- When on-site support is required, the support must be completed within four (4) business days for ASCs located in Puerto Rico, U.S. Virgin Islands, and five (5) business days for ASCs located in Hawaii, Guam, Saipan, and Alaska.

Remedial maintenance shall be performed after notification that the system is inoperative (down). The Contractor shall provide USCIS with a designated point of contact and make arrangements to enable its maintenance representative to receive such notification and provide continuous telephone coverage within the PPM to permit USCIS to make such contact (See Section 13.1, Technical Support Services (Hotline)). Within one (1) hour of notification, the Contractor shall provide a telephonic response that assesses the situation, identifies the problem, and proposes the resolution and the time to fix the problem. Resident on-site maintenance at the USCIS sites is not required.

Downtime is that time in which the Contractor maintained equipment is inoperable due to a hardware malfunction. If the failure of one device causes other devices to be inoperable, these other devices may, at the Government's option, be considered down also. A determination of downtime will be made solely by the Government. Downtime for each failure shall start at the time the Government notifies the Contractor of a failure and shall run until the failed equipment is returned to full operating condition.

Types of Coverage Required

The Contractor shall provide all maintenance coverage necessary to meet the requirements of this SOW, to include system performance requirements in SOW Section 14.0. At a minimum, the Contractor must provide remedial hardware maintenance services that meet all maintenance requirements of this SOW.

12.2.1.4 Responsibilities of the Contractor

1. Parts Quality
   The Contractor shall use only new standard parts or refurbished parts, certified as equal in performance to new parts by the Original Equipment Manufacturer, in performed repairs. Parts that have been replaced shall become the property of the Contractor. The Contractor shall maintain a replacement parts policy consistent with supporting the performance requirements as stated in this SOW.

2. Protection of Information During Equipment Maintenance

The Contractor shall prevent loss of hard drive information during all maintenance activities by taking steps to protect and, at the Government's option, restore as necessary, any information residing in the equipment being maintained. The Contractor is responsible for the erasing or wiping of information from all hard drives removed or replaced by the Contractor. Hard drives must be wiped under the supervision of the Government Computer Systems Security Officer (CSSO). The Contractor shall be responsible for notifying the Contracting Officers Technical Representative (COTR) or designated representative if a hard drive containing information has been removed from an USCIS facility without erasing the data contained on the hard drive.

3. Remote System Access for Maintenance

A VPN connection via SecureID tokens is the only means of remote system access to perform required hardware maintenance or system troubleshooting.

4. Service Incident Reports (SIRs)

The Contractor shall maintain an electronic database of all SIRs to respond to Government inquiries regarding specific problems and issues. The SIR shall contain at a minimum, the following information:

(1) Name of person requesting service
(2) Location, including site code, office, city and state/country
(3) Phone number of the person requesting service
(4) Type of equipment
(5) Serial number and USCIS property control number (PCN) of component being serviced
(6) Date and time of request for service
(7) Date and time of arrival of maintenance personnel (if applicable)
(8) Date and time replacement part shipped (if applicable)
(9) Description of problem
(10) Parts replaced (including serial number and PCN if applicable)
(11) Date and time problem was resolved
(12) Reason problem not resolved within required timeframe (if applicable)
(13) Any required follow-up actions
(14) USCIS ticket number and vendor ticket number
(15) Name of individual at affected site certifying the repair was completed

13.0 System Performance

The Contractor shall ensure that the Live-Scan systems meet the following availability and reliability requirements:

Live-Scan Systems:

- 95% availability per machine

Availability is defined as a system that is technically operational and supporting the mission of fingerprinting applicants for immigration benefits. The Live-Scan System is "unavailable" if it is unable to support the mission of capturing and transmitting complete applicant biometric data. Availability per machine is calculated as follows: number of business days/year that the machine was available divided by the number of total business days/per year x 100%. A machine is considered unavailable for one day when the machine is unavailable for over 50% of the day's total operational hours.

(Example: 255/ (365 x (5/7)) x 100% = 247/260 x 100% = **95%**)

At the Government's request, the Contractor shall replace systems that do not meet the stated requirements, above, at no cost to the Government.

13.1 Performance Deductions

The USCIS has determined that the Live-Scan equipment provided under this delivery order will perform functions that require assessment of payment deductions if the Contractor fails to correct technical malfunctions within the Government's timeframes specified below.

When on-site support is required, the Contractor shall provide all remedial action necessary to correct technical failures in Live-Scan equipment at USCIS sites within the 48 contiguous United States within three (3) business days of the trouble call, within four (4) business days for ASCs located in Puerto Rico, U.S. Virgin Islands, and five (5) business days for ASCs located in Hawaii, Guam, Saipan, and Alaska. The Contractor shall incur a $100 invoice deduction per machine per day for each machine that remains down beyond these required timeframes.

When on-site support is not required, the Contractor shall provide all remedial action necessary to correct system issues/failures in Live-Scan equipment within one (1) business day of the trouble call. The Contractor shall incur a $100 invoice deduction per machine per day for each machine that remains down beyond these required timeframes.

Availability shall be assessed by the COTR on a semi-annual basis. For each Live-Scan System found to be available less than 95% of the total operational time, an invoice deduction (taken in the following month) in the amount of $100 per machine per day over the 95% threshold shall occur.

The Contractor shall not incur deductions when Acts of God (e.g. weather), Government actions (e.g., denial of facilities access), or other events outside of Contractor control prevent the Contractor from providing remedial action within the required timeframes.

14.0 Written Deliverables/Reports

a) The Contractor shall provide a written Systems Deployment Plan in electronic format to the COTR via email no later than five (5) business days following contract award. The Systems Deployment Plan shall incorporate the deployment schedule (**Attachment D**) and address the disposal of old equipment, installation of new equipment, and training of users by USCIS Site. (**Attachment A** identifies the quantity and types of Live-Scan Systems to be installed at each USCIS location). The Systems Deployment Plan shall be in electronic format and shall not be longer than 30 pages in length.

b) The Contractor shall provide a Program Management Plan in electronic format to the COTR via email no later than five (5) business days following contract award. The Program Management Plan shall address at a minimum, a risk management plan, a communication plan, key personnel (to include résumés), and subcontractor teaming arrangements. The Program Management Plan shall not be longer than 30 pages in length.

c) The Contractor shall provide a monthly utilization report in MS Excel format to the COTR via email no later than ten (10) business days following the end of the month. This report shall detail the number of calls received, time to respond to messages, time of arrival if an on-site maintenance call, technician's name, time to resolve, length of time a machine is "unavailable", type of problem, solution, corresponding USCIS ticket number, corresponding machine's serial number, location of problem, and point of contact.

d) Prior to the commencement of deployment, the contractor shall deliver (to the COTR) via email an updated **Attachment A**, which includes the Media Access Control (MAC) addresses of each Live-Scan System to be installed at each location. The MAC addresses must be provided so that port security settings may be set by USCIS to allow for the installation of the new machines.

e) The Contractor shall provide a preventative maintenance schedule to the COTR in MS Excel format via email no later than ten (10) business days prior to performing preventative maintenance. The schedule shall identify the date of preventative maintenance for each Live-Scan System.

f) The Contractor shall provide a preventative maintenance report to the COTR in MS Excel format via email no later than ten (10) business days following the end of a preventative maintenance cycle. The report shall identify each Live-Scan System by serial number and the corresponding dates when preventative maintenance was performed.

g) The Contractor shall provide a quarterly inventory report to the COTR in MS Excel format via email no later than ten (10) business days following the end of the quarter. During the deployment of the new Live-Scan Systems, the contractor shall provide the report on a weekly-basis. The report shall consist of a list of all system locations, serial numbers, DHS Property Control Numbers (PCN), as well as IP addresses and other network information necessary to maintain the systems on the USCIS Network.

h) In Lieu of submitting individual Service Incident Reports (SIR), the Contractor shall provide a monthly Service Incident Report (SIR) that aggregates the SIRs from the month into

one report. The report shall be delivered to the COTR in MS Excel format via email no later than ten (10) business days following the end of the month.

i) The Contractor shall provide a monthly USCIS Systems Information Report to the COTR in MS Excel format via email no later than ten (10) business days following the end of the month. The report shall contain at a minimum, the following information:

1. ASC Location
2. Type (Stand Alone or Co-Located)
3. ASC Site Code (i.e. X-code)
4. Live-Scan Model
5. Live-Scan System Name
6. IP Address
7. Live-Scan System Serial Number
8. Software Version
9. Software Modified Date
10. Live-Scan System Code
11. Mail Server IP Address
12. Gateway IP Address
13. Subnet Mask
14. Network IP
15. ORI Code

j) The Contractor shall provide a monthly Service Desk Report to the COTR in MS Excel format via email no later than ten (10) business days following the end of the month. The report shall contain at a minimum, the following information:

1. Remedy Ticket Number
2. Service Desk Ticket Number
3. Date Ticket Opened
4. Date Ticket Closed
5. Number of Business Days Ticket was Open
6. System Down (Yes or No)
7. ASC Site Code (i.e. X-code)
8. ASC Site Name
9. Problem Type
10. Summary (i.e. description of problem)
11. Status (Open or Closed)

k) The Contractor shall reconcile the USCIS Remedy Monthly Report, provided to the Contractor by USCIS, with the monthly Service Desk Report on a monthly-basis and submit to the COTR via email within ten (10) business days following the receipt of the USCIS Remedy Report. The USCIS Remedy Monthly Report contains the following data:

1. Remedy Ticket Number
2. ASC Site Code (i.e. X-Code)

3. ASC Location
4. Date Ticket was Opened
5. Issue/Problem
6. Ticket Assignment (miss assigned or not)
7. Status (Open or Closed)

14.1 Written Deliverables Schedule

WRITTEN DELIVERABLES SCHEDULE

Deliverable	Due Date	Format
Systems Deployment Plan	5 business days after award	Electronic
Program Management Plan	5 business days after award	Electronic
Monthly Utilization Report	10 business days following the end of the month	MS Excel
MAC Address List	Prior to Deployment	MS Excel
Preventative Maintenance Schedule	10 business days prior to performing preventative maintenance	MS Excel
Preventative Maintenance Report	10 business days following the end of the month	MS Excel
Quarterly Inventory Report	10 business days following the end of the quarter (weekly-basis during deployment)	MS Excel
Service Incident Report	10 business days following the end of the month	MS Excel
Systems Information Report	10 business days following the end of the month	MS Excel
Monthly Service Desk Report	10 business days following the end of the month	MS Excel
Reconciled USCIS Remedy Monthly Report	10 business days following receipt of Remedy Report	MS Excel

15.0 Government Furnished Equipment (GFE)

Upon contract award and after the issuance of proper EOD clearances, the government shall provide a maximum of five (5) USCIS Laptops and five (5) SecureID VPN Tokens to the Contractor. A laptop and a VPN token each must be assigned to a single individual. The laptops and VPN tokens may only be distributed upon successful completion of the security clearance paperwork (see section 18.0 Security Requirements) resulting in a favorable Entry On Duty (EOD) determination. Additionally, the Contractor shall submit the following forms for each individual prior to attainment/use of the GFE:

- Information Technology Service Request (ITSR) Form

- USCIS HQ LAN Account Request Form
- A New Laptop User Registration Form
- USCIS VPN Request Form
- G504 Property Receiving and Acceptance Form

16.0 Electronic and Information Technology Accessibility

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable standards have been identified:

36 CFR 1194.21 – Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.
36 CFR 1194.22 – Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous Javascript and XML (AJAX) then "1194.21 Software" standards also apply to fulfill functional performance criteria.

36 CFR 1194.23 – Telecommunications Products, applies to all telecommunications products including end-user interfaces such as telephones and non end-user interfaces such as switches, circuits, etc. that are procured, developed or used by the Federal Government.

36 CFR 1194.24 – Video and Multimedia Products, applies to all video and multimedia products that are procured or developed under this work statement. Any video or multimedia presentation shall also comply with the software standards (1194.21) when the presentation is through the use of a Web or Software application interface having user controls available.

36 CFR 1194.25 – Self Contained, Closed Products, applies to all EIT products such as printers, copiers, fax machines, kiosks, etc. that are procured or developed under this work statement.
36 CFR 1194.26 – Desktop and Portable Computers, applies to all desktop and portable computers, including but not limited to laptops and personal data assistants (PDA) that are procured or developed under this work statement.

36 CFR 1194.31 – Functional Performance Criteria applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.

36 CFR 1194.41 – Information Documentation and Support, applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required "1194.31 Functional Performance Criteria", they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply:

36 CFR 1194.2(b) – (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meets some but not all of the standards, the agency must procure the product that best meets the standards.

When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires approval from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

36 CFR 1194.3(b) – Incidental to Contract, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

17.0 Facility Access Control

The Contractor shall observe all internal building security regulations that apply to any and all buildings concerned with this contract. The Contractor shall only enter the facility or building with continuous escort service. When entering and departing the facility or building each Contractor must sign in and out as required at the site.

Equipment and Materials Dismantling, Handling, and/or Hauling: The Contractor shall coordinate the route of moving equipment and materials within the facility before dismantling, handling and/or hauling same with the COTR or authorized Government representative. The Contractor shall notify the COTR or authorized Government representative to reach a mutually acceptable time and date corrective action will be completed for work required in response to an emergency or urgent service call within the response time specified herein. The Government reserves the right to inspect the equipment before, during and after any work performed.

Temporary Outages: The Contractor shall coordinate all temporary outages of any equipment with the COTR/authorized representative not less than 72 hours in advance of such outages.

18.0 Security Requirements

Prior to the commencement of work, the Contractor shall ensure that all personnel involved in the operations and maintenance service, and related work thereof, meet the security requirements identified in this SOW.

SECURITY REQUIREMENTS

GENERAL
U.S. Citizenship & Immigration Services (USCIS) has determined that performance of this contract requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor), requires access to sensitive but unclassified information, and that the Contractor will adhere to the following.

SUITABILITY DETERMINATION
USCIS shall have and exercise full control over granting, denying, withholding or terminating access to government facilities and/or access of Contractor employees to sensitive but unclassified information, based upon the results of a background investigation. USCIS may, as it deems appropriate, authorize and make a favorable entry on duty (EOD) decision based on preliminary security checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow as a result thereof. The granting of a favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by USCIS, at any time during the term of the contract. No employee of the Contractor shall be allowed unescorted access to a USCIS facility without a favorable EOD decision or suitability determination by the Office of Security and Integrity (OSI).

BACKGROUND INVESTIGATIONS

Contract employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive but unclassified information, shall undergo a position sensitivity analysis based on the duties, outlined in the Position Designation Determination (PDD) for Contractor Personnel, each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through OSI. Prospective Contractor employees shall submit the following completed forms to OSI through the COTR no less than **10** days after award of delivery order or **30** days prior to entry on duty of any employees, whether a replacement, addition, subcontractor employee, or vendor:

1. Standard Form 85P, "Questionnaire for Public Trust Positions"
2. DHS Form 11000-6, "Conditional Access to Sensitive But Unclassified Information Non-Disclosure Agreement"
3. FD Form 258, "Fingerprint Card" **(2 copies)**
4. Form DHS-11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"
5. Position Designation Determination for Contract Personnel Form
6. Foreign National Relatives or Associates Statement

Required forms will be provided by USCIS at the time of award of the contract. Only complete packages will be accepted by OSI. Specific instructions on submission of packages will be provided upon award of the contract.

Be advised that unless an applicant requiring access to sensitive but unclassified information has resided in the US for three of the past five years, OSI may not be able to complete a satisfactory background investigation. In such cases, USCIS retains the right to deem an applicant as ineligible due to insufficient background information.

The use of Non-U.S. citizens, including Lawful Permanent Residents (LPRs), is not permitted in the performance of this contract for any position that involves access to or development of any DHS IT system. USCIS will consider only U.S. Citizens for employment on this contract. USCIS will not approve LPRs for employment on this contract in any position that requires the LPR to access or assist in the development, operation, management or maintenance of DHS IT systems. By signing this contract, the contractor agrees to this restriction. In those instances where other non-IT requirements contained in the contract can be met by using LPRs, those requirements shall be clearly described.

EMPLOYMENT ELIGIBILITY

The Contractor must agree that each employee working on this contract will have a Social Security Card issued and approved by the Social Security Administration. The Contractor shall

be responsible to USCIS for acts and omissions of his own employees and for any Subcontractor(s) and their employees to include financial responsibility for all damage or injury to persons or property resulting from the acts or omissions of the contractor's employees.

Subject to existing law, regulations and/ or other provisions of this contract, illegal or undocumented aliens will not be employed by the Contractor, or with this contract. The Contractor will ensure that this provision is expressly incorporated into any and all Subcontracts or subordinate agreements issued in support of this contract.

CONTINUED ELIGIBILITY

If a prospective employee is found to be ineligible for access to USCIS facilities or information, the COTR will advise the Contractor that the employee shall not continue to work or to be assigned to work under the contract.

USCIS reserves the right and prerogative to deny and/ or restrict the facility and information access of any Contractor employee whose actions are in conflict with the standards of conduct, 5 CFR 2635 and 5 CFR 3801, or whom USCIS determines to present a risk of compromising sensitive but unclassified information to which he or she would have access under this contract.

The Contractor will report any adverse information coming to their attention concerning contract employees under the contract to USCIS OSI. The subsequent termination of employment of an employee does not obviate the requirement to submit this report. The report shall include the employees' name and social security number, along with the adverse information being reported.

OSI must be notified of all terminations/ resignations within five days of occurrence. The Contractor will return any expired USCIS issued identification cards and building passes, or those of terminated employees to the COTR. If an identification card or building pass is not available to be returned, a report must be submitted to the COTR, referencing the pass or card number, name of individual to whom issued, the last known location and disposition of the pass or card.

SECURITY MANAGEMENT

The Contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with OSI through the COTR on all security matters, to include physical, personnel, and protection of all Government information and data accessed by the Contractor.

The COTR and OSI shall have the right to inspect the procedures, methods, and facilities utilized by the Contractor in complying with the security requirements under this contract. Should the COTR determine that the Contractor is not complying with the security requirements of this delivery order, the Contractor will be informed in writing by the Contracting Officer of the proper action to be taken in order to effect compliance with such requirements.

COMPUTER AND TELECOMMUNICATIONS SECURITY REQUIREMENTS

Security Program Background

The DHS has established a department wide IT security program based on the following Executive Orders (EO), public laws, and national policy:

- Public Law 107-296, Homeland Security Act of 2002.
- Federal Information Security Management Act (FISMA) of 2002, November 25, 2002.
- Public Law 104-106, Clinger-Cohen Act of 1996 [formerly, Information Technology Management Reform Act (ITMRA)], February 10, 1996.
- Privacy Act of 1974, As Amended. 5 United States Code (U.S.C.) 552a, Public Law 93-579, Washington, D.C., July 14, 1987.
- Executive Order 12829, *National Industrial Security Program*, January 6, 1993.
- Executive Order 12958, *Classified National Security Information*, as amended.
- Executive Order 12968, *Access to Classified Information*, August 2, 1995.
- Executive Order 13231, *Critical Infrastructure Protection in the Information Age*, October 16, 2001.• National Industrial Security Program Operating Manual (NISPOM), February 2001.
- DHS *Sensitive Systems Policy Publication 4300A* v2.1, July 26, 2004
- DHS *National Security Systems Policy Publication 4300B* v2.1, July 26, 2004
- Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003.
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*.
- National Security Directive (NSD) 42, *National Policy for the Security of National Security Telecommunications and Information Systems* (U), July 5, 1990, CONFIDENTIAL.
- 5 Code of Federal Regulations (CFR) §2635, Office of Government Ethics, *Standards of Ethical Conduct for Employees of the Executive Branch*.
- DHS SCG OS-002 (IT), National Security IT Systems Certification & Accreditation, March 2004.
- Department of State 12 Foreign Affairs Manual (FAM) 600, *Information Security Technology*, June 22, 2000.
- Department of State 12 FAM 500, *Information Security*, October 1, 1999.
- Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, dated April 3, 1984.
- Presidential Decision Directive 67, *Enduring Constitutional Government and Continuity of Government Operations*, dated October 21, 1998.
- FEMA Federal Preparedness Circular 65, *Federal Executive Branch Continuity of Operations (COOP)*, dated July 26, 1999.
- FEMA Federal Preparedness Circular 66, *Test, Training and Exercise (TT&E) for Continuity of Operations (COOP)*, dated April 30, 2001.
- FEMA Federal Preparedness Circular 67, *Acquisition of Alternate Facilities for Continuity of Operations*, dated April 30, 2001.
- Title 36 Code of Federal Regulations 1236, Management of Vital Records, revised as of July 1, 2000.
- National Institute of Standards and Technology (NIST) Special Publications for computer security and FISMA compliance.

GENERAL

Due to the sensitive nature of USCIS information, the contractor is required to develop and maintain a comprehensive Computer and Telecommunications Security Program to address the

integrity, confidentiality, and availability of sensitive but unclassified (SBU) information during collection, storage, transmission, and disposal. The contractor's security program shall adhere to the requirements set forth in the DHS Management Directive 4300 IT Systems Security Pub Volume 1 Part A and DHS Management Directive 4300 IT Systems Security Pub Volume I Part B. This shall include conformance with the DHS Sensitive Systems Handbook, DHS Management Directive 11042 Safeguarding Sensitive but Unclassified (For Official Use Only) Information and other DHS or USCIS guidelines and directives regarding information security requirements. The contractor shall establish a working relationship with the USCIS IT Security Office, headed by the Information Systems Security Program Manager (ISSM).

IT SYSTEMS SECURITY

In accordance with DHS Management Directive 4300.1 "Information Technology Systems Security", USCIS Contractors shall ensure that all employees with access to USCIS IT Systems are in compliance with the requirement of this Management Directive. Specifically, all contractor employees with access to USCIS IT Systems meet the requirement for successfully completing the annual "Computer Security Awareness Training (CSAT)." All contractor employees are required to complete the training within 60-days from the date of entry on duty (EOD) and are required to complete the training yearly thereafter.

CSAT can be accessed at the following: http://otcd.uscis.dhs.gov/EDvantage.Default.asp or via remote access from a CD which can be obtained by contacting uscisitsecurity@dhs.gov.

All services provided under this delivery order must be compliant with DHS Information Security Policy, identified in MD4300.1, Information Technology Systems Security Program and 4300A Sensitive Systems Handbook.

SECURITY REVIEW

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS including the organization of the DHS Office of the Chief Information Officer, the Office of the Inspector General, authorized Contracting Officer's Technical Representative (COTR), and other government oversight organizations, access to the Contractor's facilities, installations, operations, documentation, databases, and personnel used in the performance of this contract. The Contractor will contact the DHS Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to the DHS. Access shall be provided to the extent necessary for the government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of DHS data or the function of computer systems operated on behalf of DHS, and to preserve evidence of computer crime.

IT SECURITY IN THE SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC)

The USCIS SDLC Manual documents all system activities required for the development, operation, and disposition of IT security systems. Required systems analysis, deliverables, and security activities are identified in the SDLC manual by lifecycle phase. The contractor shall assist the appropriate USCIS ISSO with development and completion of all SDLC activities and deliverables contained in the SDLC. The SDLC is supplemented with information from DHS

and USCIS Policies and procedures as well as the National Institute of Standards Special Procedures related to computer security and FISMA compliance. These activities include development of the following documents:

- *Sensitive System Security Plan (SSSP)*: This is the primary reference that describes system sensitivity, criticality, security controls, policies, and procedures. The SSSP shall be based upon the completion of the DHS FIPS 199 workbook to categorize the system of application and completion of the RMS Questionnaire. The SSSP shall be completed as part of the System or Release Definition Process in the SDLC and shall not be waived or tailored.
- *Privacy Impact Assessment (PIA) and System of Records Notification (SORN).* For each new development activity, each incremental system update, or system recertification, a PIA and SORN shall be evaluated. If the system (or modification) triggers a PIA the contractor shall support the development of PIA and SORN as required. The Privacy Act of 1974 requires the PIA and shall be part of the SDLC process performed at either System or Release Definition.
- *Contingency Plan (CP)*: This plan describes the steps to be taken to ensure that an automated system or facility can be recovered from service disruptions in the event of emergencies and/or disasters. The Contractor shall support annual contingency plan testing and shall provide a Contingency Plan Test Results Report.
- *Security Test and Evaluation (ST&E)*: This document evaluates each security control and countermeasure to verify operation in the manner intended. Test parameters are established based on results of the RA. An ST&E shall be conducted for each Major Application and each General Support System as part of the certification process. The Contractor shall support this process.
- *Risk Assessment (RA):* This document identifies threats and vulnerabilities, assesses the impacts of the threats, evaluates in-place countermeasures, and identifies additional countermeasures necessary to ensure an acceptable level of security. The RA shall be completed after completing the NIST 800-53 evaluation, Contingency Plan Testing, and the ST&E. Identified weakness shall be documented in a Plan of Action and Milestone (POA&M) in the USCIS Trusted Agent FISMA (TAF) tool. Each POA&M entry shall identify the cost of mitigating the weakness and the schedule for mitigating the weakness, as well as a POC for the mitigation efforts.
- *Certification and Accreditation (C&A):* This program establishes the extent to which a particular design and implementation of an automated system and the facilities housing that system meet a specified set of security requirements, based on the RA of security features and other technical requirements (certification), and the management authorization and approval of a system to process sensitive but unclassified information (accreditation). As appropriate the Contractor shall be granted access to the USCIS TAF and Risk Management System (RMS) tools to support C&A and its annual assessment requirements. Annual assessment activities shall include completion of the NIST 800-26 Self Assessment in TAF, annual review of user accounts, and annual review of the FIPS categorization. C&A status shall be reviewed for each incremental system update and a new full C&A process completed when a major system revision is anticipated.

SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

(1) Within 30 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

(3) The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(c) Examples of tasks that require security provisions include--

(1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and

(2) Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).

(d) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract, and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A

(Version 5.5, September 30, 2007) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

CONTRACTOR EMPLOYEE ACCESS

(a) *Sensitive Information*, as used in this Chapter, means any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to

determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the contractor to prohibit individuals from working on the contract if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, and insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those contractor employees authorized access to sensitive information, the contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(g) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Technical Representative (COTR) will arrange, and complete any nondisclosure agreement furnished by DHS.

(h) The contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract. Any attempts by contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the contractor performs business for the DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a